

REMARKS/ARGUMENTS

In response to the Examiner's final Office Action of September 13, 2007 issued with respect to the present RCE application, the Applicant respectfully submits the accompanying Request for Continued Examination and Amendment of the claims, and the below Remarks.

Regarding Amendment

In the Amendment:

independent claim 1 is amended to designate the random number encrypted by the symmetric encryption function using the second key in the trusted chip as a second number and to clarify that, in the test function, the first number is first received a plural and random number of times, the comparison with the first number is performed up to this number of times and should return a mismatch with the trusted chip, that if a mismatch is not returned by the current comparison then the trusted chip is invalid and the protocol is terminated, and that if all of the comparisons with the first number return a mismatch then the comparison with the second number is performed. Support for these amendments can be found, for example, at page 50, line 30-page 52, line 15 and page 66, line 17-page 67, line 3 of the present specification; and

dependent claims 2, 4, 5, 7-14 and 16-20 are unchanged.

It is respectfully submitted that the Amendment does not add any new matter to the present application.

Regarding Examiner's Note

It is respectfully submitted that the above-described amendments of independent claim 1 make it clear that the "trusted" chip is considered to be trusted so long as each call of the test function using the first number returns a mismatch, as is described at page 66, line 17-page 67, line 3 of the present specification.

Regarding 35 USC 112, second paragraph Rejections

It is respectfully submitted that amended independent claim 1 clearly recites all possible outcomes of the comparisons performed by the test function and clarifies the use of the "second number" in the comparisons.

Regarding 35 USC 103(a) Rejections

It is respectfully submitted that the subject matter of amended independent claim 1, and claims 2, 4, 5, 7-14 and 16-20 dependent therefrom, is not taught or suggested by any one or more of previously cited Carmon, Sony, Spies and Schneier in view of newly cited Goto (US 5,617,429), for at least the following reasons.

Independent claim 1 has been amended to emphasise that the test function is called a plural and random number of times with the wrong hash value so as to test the validity of the trusted chip before the validity of the untrusted chip is tested. In this way, clone trusted chips which are manufactured to always return a valid result from the test function or to return a valid result after a preselected number of test function calls can be reliably detected (see page 66, line 17-page 67, line 3 of the present specification).

As admitted by the Examiner, none of Carmon, Sony, Spies and Schneier teach or suggest calling a test function of a trusted authentication chip with a wrong hash value.

Further, Goto merely discloses a self-test in which the signal conductor 81 is selected to be at a high or low level in order to selectively apply an intentionally wrong expected value to the comparator 6, which enables judgement of whether or not the failure detection system is operating normally (see col. 16, lines 21-58).

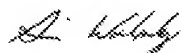
Goto does not teach applying the wrong expected value a plural and random number of times before applying the values to be tested by the failure detection system, as would be required to meet the claimed invention. Furthermore, there is no suggestion from the disclosure of Goto to do this because one of ordinary skill in the art understands from the disclosure of Goto that performing the self-test a consecutive number of times with the same wrong expected value would not achieve any different result to performing the self-test once only.

Thus, the subject matter of amended independent claim 1, and claims 2, 4, 5, 7-14 and 16-20 dependent therefrom, is not taught or suggested by Carmon, Sony, Spies, Schneier and Goto either taken alone or in combination with one another.

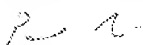
It is respectfully submitted that all of the Examiner's objections and rejections have been traversed. Accordingly, it is submitted that the present application is in condition for allowance and reconsideration of the present application is respectfully requested.

Very respectfully,

Applicant/s:



Simon Robert Walmsley



Paul Lapstun

C/o: Silverbrook Research Pty Ltd
393 Darling Street
Balmain NSW 2041, Australia

Email: kia.silverbrook@silverbrookresearch.com

Telephone: +612 9818 6633

Facsimile: +61 2 9555 7762